CLAIMS

1. A method comprising:

receiving a request to transfer application data from a source computing device to a destination computing device;

checking whether the application data can be transferred to the destination computing device, and if so, then checking whether the application data can be transferred under control of the user or a third party; and

receiving input from the appropriate one of the user or third party to control transferring of the application data to the destination computing device.

2. A method as recited in claim 1, further comprising:

checking whether the destination computing device is trusted to receive the application data; and

preventing the application data from being transferred if the destination computing device is not trusted to receive the application data.

3. A method as recited in claim 2, wherein checking whether the destination computing device is trusted to receive the application data comprises checking whether software executing on the destination computing device is trusted to receive the application data.

4. A method as recited in claim 2, wherein checking whether the destination computing device is trusted to receive the application data comprises the third party checking whether the destination computing device is trusted to receive the application data.

5. A method as recited in claim 2, wherein checking whether the destination computing device is trusted to receive the application data comprises having another party check, on behalf of the source computing device, whether the destination computing device is trusted to receive the application data.

6. A method as recited in claim 1, wherein checking whether the application data can be transferred comprises checking whether the application data is non-migrateable, user-migrateable, or third party-migrateable.

7. A method as recited in claim 6, further comprising:

if the application data is non-migrateable, then not allowing the application secret to be transferred;

if the application data is user-migrateable, then allowing the application secret to be transferred under control of a user; and

if the application data is third party-migrateable, then allowing the application secret to be transferred under control of a third party.

8. A method as recited in claim 6, wherein, if the application data is user-migrateable, then:

receiving input from the appropriate one of the user or third party comprises identifying a user passphrase;

the method further comprising:

identifying an encryption key previously used to encrypt the application data, wherein the encryption key corresponds to user-migrateable data,

encrypting the encryption key based at least in part on the user passphrase, and

allowing the encrypted encryption key to be copied to the destination computing device.

9. A method as recited in claim 6, wherein, if the application data is third party-migrateable, then:

receiving input from the appropriate one of the user or third party comprises identifying a public key of a public-private key pair associated with the third party;

the method further comprising:

identifying an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to third party-migrateable data,

encrypting the encryption key based at least in part on the public key, and

allowing the encrypted encryption key to be copied to the destination computing device.

10. A method as recited in claim 1, further comprising:

receiving application data to be encrypted and stored on the source computing device;

identifying how the application data is to be allowed to be transferred to the destination computing device if a request to transfer the application data is received; and

selecting a particular one of a plurality of encryption keys to encrypt the application data, wherein the selecting is based at least in part on how the application data is to be allowed to be transferred to another computing device.

11. A method as recited in claim 1, further comprising:

allowing application data for a plurality of applications to be transferred to the destination computing device by moving a single key to the destination computing device.

12. A method, implemented on a computing device, the method comprising:

generating a gatekeeper storage key;

sealing the gatekeeper storage key to a trusted core executing on the computing device;

receiving a request to store an application secret;

receiving a type of the application secret;

selecting an appropriate hive key based at least in part on the type of the application secret;

encrypting the application secret using the hive key; and

encrypting the hive key using the gatekeeper storage key.

13. A method as recited in claim 12, wherein selecting the appropriate hive key comprises:

checking whether a hive key corresponding to the type of the application secret already exists;

if the hive key does not already exist, then creating a hive key corresponding to the type of the application secret and selecting the newly created hive key; and

if the hive key does already exist, then selecting the already existing hive key.

14. A method as recited in claim 12, wherein selecting the appropriate hive key comprises:

selecting an appropriate hive key based at least in part on both the application from which the request is received and the type of the application secret.

15. A method as recited in claim 12, wherein selecting the appropriate hive key further comprises selecting different hive keys for different application secrets received from the same application.

16. A method as recited in claim 12, wherein the type of the application secret comprises one of: a non-migrateable secret, a user-migrateable secret, and a third party-migrateable secret.

17. A method as recited in claim 12, further comprising:

receiving a request to transfer the encrypted application secret to another computing device; and

determining whether to allow the encrypted application secret to be transferred to another computing device based at least in part on the type of the application secret.

18. A method as recited in claim 17, wherein the determining comprises:

if the type of the application secret is non-migrateable, then not allowing the application secret to be transferred;

if the type of the application secret is user-migrateable, then allowing the application secret to be transferred under control of a user; and

if the type of the application secret is third party-migrateable, then allowing the application secret to be transferred under control of a third party.

19. A method as recited in claim 12, wherein receiving the request to store an application secret comprises:

receiving, from a trusted application executing on the computing device, a request to store an application secret.

20. One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a source computing device, causes the one or more processors to:

receive a request to transfer an application secret from the source computing device to a destination computing device;

identify a type of the application secret;

if the type is non-migrateable, then not allow the application secret to be transferred;

if the type is user-migrateable, then allow the application secret to be transferred under control of a user; and

if the type is third party-migrateable, then allow the application secret to be transferred under control of a third party.

21. One or more computer readable media as recited in claim 20, wherein the plurality of instructions to allow the application secret to be transferred under control of the user comprises a plurality of instructions to:

identify a user passphrase;

identify an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to the user-migrateable type;

encrypt the encryption key based at least in part on the user passphrase; and

allow the encrypted encryption key to be copied to the destination computing device.

22. One or more computer readable media as recited in claim 21, wherein the plurality of instructions to identify the user passphrase comprises a plurality of instructions to:

query the user for the passphrase; and

identify, as the passphrase, an input from the user in response to the query.

23. One or more computer readable media as recited in claim 20, wherein the plurality of instructions to allow the application secret to be transferred under control of the third party comprises a plurality of instructions to:

identify a public key of a public-private key pair associated with the third party;

identify an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to the third party-migrateable type;

encrypt the encryption key based at least in part on the public key; and

allow the encrypted encryption key to be copied to the destination computing device.

24. One or more computer readable media as recited in claim 20, wherein the plurality of instructions further cause the one or more processors to:

receive, from another computing device, a plurality of additional application secrets, wherein each of the additional application secrets is encrypted;

identify a first group of the plurality of additional application secrets that are to be decrypted under user control;

obtain, from the user, a passphrase; and

use the passphrase to decrypt each encrypted application secret of the first group.

25. One or more computer readable media as recited in claim 24, wherein the plurality of instructions further cause the one or more processors to:

identify a second group of the plurality of additional application secrets that are to be decrypted under third party control; and

communicate with a third party to have each encrypted application secret of the second group decrypted.

26. One or more computer readable media as recited in claim 20, wherein the third party comprises a smartcard.

27. One or more computer readable media as recited in claim 20, wherein the plurality of instructions further cause the one or more processors to:

authenticate the destination computing device as being trusted to receive the application secret; and

preventing the application secret from being transferred if the destination computing device is not trusted to receive the application secret.

28. One or more computer readable media as recited in claim 20, wherein the plurality of instructions further comprise instructions that cause the one or more processors to:

allow a plurality of application secrets to be transferred under control of the user by using a single key associated with the user-migrateable type.

29. One or more computer readable media as recited in claim 20, wherein the plurality of instructions further comprise instructions that cause the one or more processors to:

allow a plurality of application secrets to be transferred under control of the third party by using a single key associated with the third party-migrateable type.

30. One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a computing device, causes the one or more processors to:

receive application data to be encrypted and stored;

identify how the application data is to be allowed to be transferred to another computing device if a request to transfer the application data is received; and

select a particular one of a plurality of encryption keys to encrypt the application data, wherein the selecting is based at least in part on how the application data is to be allowed to be transferred to another computing device.

31. One or more computer readable media as recited in claim 30, wherein the plurality of instructions that cause the one or more processors to select the particular one of the plurality of encryption keys comprise instructions to:

check whether an encryption key corresponding to a type of the application data already exists;

if the encryption key does not already exist, then create an encryption key corresponding to the type of the application data and select the newly created encryption key; and

if the encryption key does already exist, then selecting the already existing encryption key.

32. One or more computer readable media as recited in claim 30, wherein:

the application data comprises one of: non-migrateable data, user-migrateable data, and third party-migrateable data.

33. One or more computer readable media as recited in claim 30, further comprising instructions that, when executed by the one or more processors, cause the one or more processors to:

receive a request to transfer the encrypted application data to another computing device; and

determine whether to allow the encrypted application data to be transferred to the other computing device based at least in part on whether the application data is non-migrateable data, user-migrateable data, or third party-migrateable data.

34. One or more computer readable media as recited in claim 33, wherein the instructions to determine whether to allow the encrypted application data to be transferred to the other computing device comprises instructions that, when executed by the one or more processors, cause the one or more processors to:

if the application data is non-migrateable, then not allow the application secret to be transferred;

if the application data is user-migrateable, then allow the application secret to be transferred under control of a user; and

if the application data is third party-migrateable, then allow the application secret to be transferred under control of a third party.

35. One or more computer readable media as recited in claim 30, wherein the application data is received from a trusted application executing on the computing device.

36. A system comprising:

a processor; and

a memory, coupled to the processor, to store a plurality of instructions that, when executed by the processor, causes the processor to,

receive an application secret to be securely stored,

identify a secret type that indicates how the application secret is to be allowed to be transferred to another system if a request to transfer the application secret is received, and

select a particular one of a plurality of encryption keys to encrypt the application secret, wherein the selecting is based at least in part on the secret type.

37. A system as recited in claim 36, wherein the plurality of instructions that cause the processor to select the particular one of the plurality of encryption keys comprise instructions to:

check whether an encryption key corresponding to the type of the application secret already exists;

if the encryption key does not already exist, then create an encryption key corresponding to the type of the application secret and select the newly created encryption key; and

if the encryption key does already exist, then selecting the already existing encryption key.

38. A system as recited in claim 36, wherein:

the secret type comprises one of: a non-migrateable secret, a user-migrateable secret, and a third party-migrateable secret.

39. A system as recited in claim 36, wherein the memory further stores instructions that, when executed by the processor, cause the processor to:

receive a request to transfer the encrypted application secret to another system; and

determine whether to allow the encrypted application data to be transferred to the other system based at least in part on the secret type.

40. A system as recited in claim 39, wherein the instructions to determine whether to allow the encrypted application data to be transferred to the other system comprises instructions that, when executed by the processor, cause the processor to:

if the secret type is non-migrateable, then not allow the application secret to be transferred;

if the secret type is user-migrateable, then allow the application secret to be transferred under control of a user; and

if the secret type is third party-migrateable, then allow the application secret to be transferred under control of a third party.

41. One or more computer readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a computing device, causes the one or more processors to:

receive a plurality of encrypted application secrets from another computing device;

identify a first group of the plurality of encrypted application secrets that are to be decrypted under user control;

obtain, from a user, a passphrase;

use the passphrase to decrypt each encrypted application secret of the first group of encrypted application secrets;

identify a second group of the plurality of encrypted application secrets that are to be decrypted under third party control; and

communicate with a third party to have each encrypted application secret of the second group of encrypted application secrets decrypted.

42. One or more computer readable media as recited in claim 41, wherein each encrypted application secret of the first group comprises a user-migrateable application secret, and wherein each encrypted application secret of the second group comprises a third party-migrateable application secret.

43. One or more computer readable media having stored thereon a plurality of instructions for backing up data on a computing device, wherein the plurality of instructions, when executed by one or more processors of the computing device, causes the one or more processors to:

check, for an application secret to be backed up, a type of the application secret;

if the application secret type is non-migrateable, then not allow the application secret to be transferred to a backup medium;

if the application secret type is user-migrateable, then encrypt the application secret based at least in part on a passphrase and allow the encrypted application secret to be transferred to the backup medium; and

if the application secret type is third party-migrateable, then encrypt the application secret based at least in part on a third party key and allow the encrypted application secret to be transferred to the backup medium.

44. One or more computer readable media as recited in claim 43, wherein the instructions the instructions to encrypt the application secret based at least in part on the passphrase and allow the encrypted application secret to be transferred to the backup medium, cause the one or more processors to:

identify a user passphrase;

identify an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to the user-migrateable type;

encrypt the encryption key based at least in part on the user passphrase; and

allow the encrypted encryption key to be transferred to the backup medium.

45. One or more computer readable media as recited in claim 43, wherein the instructions the instructions to encrypt the application secret based at least in part on the third party key and allow the encrypted application secret to be transferred to the backup medium, cause the one or more processors to:

identify a public key of a public-private key pair associated with the third party;

identify an encryption key previously used to encrypt the application secret, wherein the encryption key corresponds to the third party-migrateable type;

encrypt the encryption key based at least in part on the public key; and

allow the encrypted encryption key to be transferred to the backup medium.

46. One or more computer readable media as recited in claim 43, wherein the plurality of instructions, when executed by the one or more processors, further causes the one or more processors to:

receive, from another computing device, a plurality of additional application secrets, wherein each of the additional application secrets is encrypted;

identify a first group of the plurality of additional application secrets that are to be decrypted under user control;

obtain, from the user, a passphrase; and

use the passphrase to decrypt each encrypted application secret of the first group.

47. One or more computer readable media as recited in claim 46, wherein the plurality of instructions, when executed by the one or more processors, further causes the one or more processors to:

identify a second group of the plurality of additional application secrets that are to be decrypted under third party control; and

communicate with a third party to have each encrypted application secret of the second group decrypted.

48. One or more computer readable media as recited in claim 43, wherein the third party key corresponds to a third party, and wherein the third party comprises a smartcard.

49. A method comprising:

receiving a request to transfer a plurality of application secrets from a source computing device to a destination computing device;

identifying which one of a plurality of types of application secrets the plurality of application secrets correspond to;

identifying a key associated with the one type;

allowing the plurality of application secrets to be accessible to the destination computing device by communicating the key to the destination computing device.

50. A method as recited in claim 49, wherein the type of application secret is all secrets and the key associated with the one type is a gatekeeper storage key.

51. A method as recited in claim 49, wherein the key comprises a hive key.